

LISTING OF CLAIMS

1. (currently amended) A method for prohibiting access to a computer, having a radio frequency identification (RFID) chip and capable of having a removable radio frequency (RF) antenna security device installed therein, after a radio frequency antenna security device has been removed from said computer, comprising the steps of:

(a) storing data comprising at least an antenna history, antenna error, detect coil, detect enable, tamper and access protection bit regions indicating that said security device was originally attached to said computer in a first region of first storage means at said RF chip in said computer, wherein said first storage means is capable of storing data received from said RF antenna while a main power source of said computer is turned off;

(b) starting a procedure for prohibiting the access to change said stored data at said computer following the completion of said step (a);

(c) using said data stored in said first region to verify that said security device was once attached to said computer by accessing at least said antenna history bit;

(d) dynamically determining that said security device is no longer attached to said computer; and

JP919980227

-2-

(e) prohibiting the access to said computer in response to said steps (c) and (d).

2. (original) The method according to claim 1, wherein said step (b) is initiated in response to a trigger event.

3. (original) The method according to claim 1, wherein said step (e) is performed only when an authorized password is not entered.

4. (previously presented) The method according to claim 3, further comprising the step of:

storing, in response to receipt of an authorized password, data indicating that said security device that was once attached to said computer has been removed in a second region of said first storage means.

5-11 (canceled)

12. (previously presented) A computer, having a radio frequency identification (RFID) chip, capable of having a removable radio frequency (RF) antenna security device installed therein, comprising:

first storage means at said RFID chip capable of storing data received from said RF antenna while a main power source of said computer is turned off; a central processing unit; means for storing data comprising at least antenna history, antenna error, detect coil, detect enable, tamper and access protection bit regions indicating that said security device that was once attached to said computer has been removed therefrom in a region of the first storage means; detection means for using said data stored in said region to detect that said security device attached to said computer has been removed therefrom; and means for prohibiting, in response to said detection means, access to said computer.

13-20 (canceled)

21. (previously presented) The computer according to claim 12 further comprising means for determining if removal of said security device was authorized and means for storing, in response to said determination data indicating that said security device that was once attached to said

computer has been legitimately removed therefrom in a second region of said first storage means.

22-24 (canceled)

25. (previously presented) The computer according to claim 12, wherein said RF antenna is attached to a lid of a device bay of said computer.

26-27 (canceled)

28. (previously presented) The method according to claim 1 wherein said storing is done in response to receipt of an RF excitation signal received from a remote RF transmitter.

29-30 (canceled)

JP91998Q227

-5-